CLAIMS

What is claimed is:

1. A computer-implemented method for managing sensitive data in a point-of-sale terminal having a first memory element, a processor having a register, a security circuit, and a power supply circuit arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source, comprising:

storing sensitive data in the first memory element;

upon loss of power from the first source, switching to power from the second source, copying the sensitive data from the first memory element to the register, and erasing the sensitive data from the first memory element; and

upon detecting an attack on the terminal, erasing the sensitive data from the first memory element and from the register.

2. The method of claim 1, further comprising upon reapplication of power from the first source, copying the sensitive data from the register to the RAM.

3. The method of claim 2, wherein the sensitive data includes a general encryption key.

4. The method of claim 3, wherein the first memory element is RAM internal to the processor, and the terminal further includes a second memory element that is a RAM external to the processor, the method further comprising:

generating encrypted data using the general encryption key; and storing the encrypted data in the second memory element.

5. The method of claim 4, further comprising:

generating a random value;

storing the random value in the first memory element;

encrypting the random value as a marker value using the general encryption key;

storing the marker value in the second memory element; and

upon application of power from the first source, generating a temporary marker value from the random value stored in the first memory element and the general encryption key, wherein an attack is detected if the temporary marker value is not equal to the marker value in the second memory element.

6. The method of claim 1, wherein the sensitive data includes a general encryption key.

7. The method of claim 6, wherein the first memory element is RAM internal to the processor, and the terminal further includes a second memory element that is a RAM external to the processor, the method further comprising:

generating encrypted data using the general encryption key; and

storing the encrypted data in the second memory element.

8. The method of claim 7, further comprising:

generating a random value;

storing the random value in the first memory element;

encrypting the random value as a marker value using the general encryption key;

storing the marker value in the second memory element; and

upon application of power from the first source, generating a temporary marker value from the random value stored in the first memory element and the general encryption key, wherein an attack is detected if the temporary marker value is not equal to the marker value in the second memory element.

9. An apparatus for managing sensitive data in a point-of-sale terminal having a first memory element, a processor having a register, a security circuit, and a power supply circuit arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source, comprising:

means for storing sensitive data in the first memory element;

means, responsive to a loss of power from the first source, for switching to power from the second source, copying the sensitive data from the first memory element to the register, and erasing the sensitive data from the first memory element; and

means for detecting an attack on the terminal; and

means for erasing the sensitive data from the first memory element and from the register in response to an attack on the terminal.

10. A circuit arrangement providing for erasure of sensitive data, comprising:

a first memory element;

a register;

a security circuit configured to detect a security threat to the circuit arrangement and generate a first signal upon detection of a security threat;

a power supply coupled to the first memory element, the register, and the security circuit, the power supply arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source; and

a processor coupled to the RAM, the register, the security circuit and the power supply, the processor configured to store sensitive data in the RAM when power is available from the first source, and upon application of power from the second power source copy the sensitive data from the RAM to the register and erase the sensitive data from the RAM.

11 The circuit arrangement of claim 10, wherein the processor is further configured to copy the sensitive data from the register to the RAM upon reapplication of power from the first source.

12. The circuit arrangement of claim 11, wherein the sensitive data includes a general encryption key.

13. The circuit arrangement of claim 12, wherein the first memory element is RAM internal to the processor, and further comprising:

a second memory element that is a RAM external and coupled to the processor; and

wherein the processor is further configured to generate encrypted data using the general encryption key and store the encrypted data in the second memory element.

14. The circuit arrangement of claim 13, wherein the processor is further configured to generate a random value and store the random value in the first memory element, encrypt the random value as a marker value using the general encryption key and store the marker value in the second memory element, and upon application of power from the first source, generate a temporary marker value from the random value stored in the first memory element and the general encryption key, detect an attack if the temporary marker value is not equal to the marker value in the second memory element.